UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,088	12/18/2001	Roy Want	42390P12019	4912

45209 7590 08/31/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
ZEWARI, SAYED T	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
08/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/025,088	WANT ET AL.	
	Examiner	Art Unit	
	SAYED T. ZEWARI	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-15 and 17-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-15, 17-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments filed on 12/19/2008 have been fully considered but they are not persuasive.

2. Applicant argues

> *Applicant submits that neither Kiessling nor Proust disclose or suggest a controller establishing a wireless communication link with a first remote device based upon a determination that services offered by a remote device are relevant. The Office Action asserts that Kiessling at col. 5, 11. 17-40 discloses such a process. See Office Action at Page 4, lines 7-11. Applicant respectfully disagrees.*

This argument is not persuasive. Kiessling discloses in figure 2, a controller (25) which controls communication modules (RF circuitry, Bluetooth circuitry, IR circuitry). These communication modules establish wireless connection to remote devices.

Applicant further argues

> *Applicant submits that nowhere in the above passage is there disclosed, or reasonably suggested, a controller establishing a wireless communication link with a remote device based* ***upon a determination that services offered by a first remote device are relevant.***

This argument is not persuasive. As mentioned above, Kiessling discloses in figure 2, a controller (25) which controls communication modules (RF circuitry, Bluetooth circuitry, IR circuitry). These communication modules establish wireless connection to remote

devices. The establishment of communication between these communication module and remote devices are necessarily based on a determination that those remote has some services about which they want to communicate.

3. Applicant argues

> *Moreover, applicant submits that Kiessling and Proust also fail to disclose or suggest the controller granting access rights to a public storage area and a private storage area based on a classification of a first remote device. The Office Action asserts that Proust discloses that selected remote devices exchange data in restricted manner. See Office Action at Page 4, lines 11-17. Notwithstanding the Examiner's assertion, there is no disclosure of a process of granting access rights to a public storage area and a private storage area based on a classification of a first remote device.*

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

4. Kiessling also discloses a portable device that includes a wireless communication, a data storage module, and a controller that controls the access of remote devices to the public data storage area of the portable device.

5. Proust also discloses a portable device with wireless module, controller and data storage module. The controller controls the access of remote devices to the data storage area.

6. Therefore, the applied references disclose all the limitations of the claims of the applicant.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3-8, 10-12, 15, 17-29, and 31-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiessling et al. (US 6,901,251) in view of Proust et al. (US 6,216,014).

With respect to claim 1, Kiessling discloses a portable wireless device **(See Kiessling's abstract, figure 1(1), col.3 lines 44-45 see additional info: col.3 lines 46-67, col.4 lines 1-11)** which includes a wireless communication module to communicate with each of a plurality of remote devices within a locality **(See Kiessling's figure 2(30,31,32), col.4 lines 34-48)**; a data storage module having a public storage area with which selected remote devices exchange data in a free manner **(See Kiessling's figure 2(24), col.1 lines 15-21 where remote devices can access the applications on local storage),** a controller connected to the wireless communication module and to the data storage module **(See Kiessling's figure 2(25**

&23), col.4 lines 15-18, col.1 lines 15-21), to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area based on a classification of the first remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**. Kiessling discloses everything claimed as applied above to claim 1, except for explicitly reciting the use of a private storage area with which selected remote devices exchange data in a restricted manner. In analogous art, Proust et al. discloses the use of a private area with which selected remote devices exchange data in a restricted manner **(See Proust's figure 1(8), col.11 lines 14-18, figure 3 col.11 lines 41-47, col.12 lines 30-38, figure 4 col.12 lines 39-67, col.13 lines 1-11).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by including a separate data storage area for storing restricted data where access to this data is controlled in order to improve security of data, as taught by Proust et al. **(See Proust's col.3 lines 22-31).**

With respect to claim 15, Kiessling discloses a data communication system **(See Kiessling's abstract, figure 1, col.3 lines 44-45)**, which includes: a plurality of remote devices, each remote device including a wireless communication interface **(See Kiessling's abstract, figure 1, col.3 lines 44-45)**; and at least one portable device **(See Kiessling's abstract, figure 1, col.3 lines 44-45, figure 2)**, which includes: a wireless communication module to communicate within a locality with the wireless communication interface the remote devices **(See Kiessling's figure 2, col.4 lines 34-**

48); a data storage module having a public storage area with which selected remote devices exchange data in a free manner **(See Kiessling's figure 2(24), col.1 lines 15-21 where remote devices can access the applications on local storage)** a controller connected to the wireless communication module and to the data storage module **(See Kiessling's figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21)**, to establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and to grant access rights to the public storage area based on a classification of the first remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**. Kiessling discloses everything claimed as applied above to claim 15, except for explicitly reciting the use of a private storage area with which selected remote devices exchange data in a restricted manner. In analogous art, Proust et al. discloses the use of a private area with which selected remote devices exchange data in a restricted manner **(See Proust's figure 1(8), col.11 lines 14-18, figure 3 col.11 lines 41-47, col.12 lines 30-38, figure 4 col.12 lines 39-67, col.13 lines 1-11).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by including a separate data storage area for storing restricted data where access to this data is controlled in order to improve security of data, as taught by Proust et al. **(See Proust's col.3 lines 22-31).**

With respect to claim 21, Kiessling discloses a method which includes: monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality

(See Kiessling's figure 2, col.4 lines 34-48), the portable device including a public storage area with which selected remote devices exchange data in a free manner **(See Kiessling's figure 2(24), col.1 lines 15-21 where remote devices can access the applications on local storage)**, identifying access rights associated with the remote device **(See Kiessling's figure 2(25), col.4 lines 15-18, col.1 lines 15-21)**; establishing a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant; and granting access rights to the public storage area based on a classification of the first remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**. Kiessling discloses everything claimed as applied above to claim 21, except for explicitly reciting the use of a private storage area with which selected remote devices exchange data in a restricted manner. In analogous art, Proust et al. discloses the use of a private area with which selected remote devices exchange data in a restricted manner **(See Proust's figure 1(8), col.11 lines 14-18, figure 3 col.11 lines 41-47, col.12 lines 30-38, figure 4 col.12 lines 39-67, col.13 lines 1-11).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by including a separate data storage area for storing restricted data where access to this data is controlled in order to improve security of data, as taught by Proust et al. **(See Proust's col.3 lines 22-31).**

With respect to claim 33, Kiessling discloses a computer program product including a medium readable by a computer **(See Kiessling's figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21)**, the medium carrying instructions which, when executed

by the computer, cause the computer to: monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor **(See Kiessling's figure 2, col.4 lines 34-48)**, and a data storage module a public storage area with which selected remote devices exchange data in a free manner **(See Kiessling's figure 2(24), col.1 lines 15-21 where remote devices can access the applications on local storage)**, and; identify access rights associated with the remote device **(See Kiessling's figure 2(25), col.4 lines 15-18, col.1 lines 15-21)**; and establish a wireless communication link between the wireless communication module and a first remote device upon a determination that services offered by the first remote device are relevant and granting access rights to the public storage area based on a classification of the first remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**. Kiessling discloses everything claimed as applied above to claim 33, except for explicitly reciting the use of a private storage area with which selected remote devices exchange data in a restricted manner. In analogous art, Proust et al. discloses the use of a private area with which selected remote devices exchange data in a restricted manner **(See Proust's figure 1(8), col.11 lines 14-18, figure 3 col.11 lines 41-47, col.12 lines 3038, figure 4 col.12 lines 39-67, col.13 lines 1-11).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by including a separate data storage area for storing restricted data where access to this data is controlled in order to improve security of data, as taught by Proust et al. **(See Proust's col.3 lines 22-31).**

With respect to claim 3, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses a controller filters requests from each of the remote devices to exchange data and to reject and accept the requests in response to the nature of services offered by the remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 4, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses a controller that defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 5, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area **(See Kiessling's col.3 lines 17-20, claim 2 col.7 lines 34-37)**.

With respect to claim 6, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses the controller restricts how often and the amount of data which is writable by the remote device into the public storage area **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21)**

With respect to claim 7, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses that data stored in the public storage area is selectively cleared by the controller in an automated fashion **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21).**

With respect to claim 8, Kiessling discloses everything as applied to claim 1 including use of security protocol (figure 2 (39), col.5 lines 10-15). However, Kiessling does not specifically recite the use of a SSL (Secure Sockets Layer). The applicant, however, has admitted, the use of SSL protocol was well known and expected in the art for the purpose of securing communication lines **(See applicant's specification page 7 lines 17-19)**. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by using the well known SSL protocol as the security protocol for Kiessling's mobile device, for the purpose of enabling secure communication as admitted by the applicant.

With respect to claim 10, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses that the wireless communication module is a radio frequency (RF) transceiver which communicates using a standardized communication protocol **(See Kiessling's figure 2(30 &31), col.4 lines 34-48).**

With respect to claim 11, Kiessling discloses everything as applied to claim 10. Additionally Kiessling discloses that the standardized communication protocol is selected from the group including Bluetooth IEEE 802.15 technology, IEEE 802.1 l a technology, and IEEE 802.1lb technology **(See Kiessling's figure 2(31), col.4 lines 34-48).**

With respect to claim 12, Kiessling discloses everything as applied to claim 1. Additionally Kiessling discloses that the controller interfaces the portable device to a computer system **(See Kiessling's figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-**

21) to permit a user to access and store data in the data storage module **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 17, Kiessling discloses everything as applied to claim 15. Additionally Kiessling discloses that the controller filters requests from each of the remote devices to exchange data and to selectively reject and accept the requests in response to the nature of services offered by the remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 18, Kiessling discloses everything as applied to claim 15. Additionally Kiessling discloses that the controller defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 19, Kiessling discloses everything as applied to claim 15. Additionally Kiessling discloses that a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area **(See Kiessling's col.3 lines 17-20, claim 2 col.7 lines 34-37)**.

With respect to claim 20, Kiessling discloses everything as applied to claim 15. Additionally Kiessling discloses that the controller restricts the amount of data which is writable by the remote device into the public storage area **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21).**

With respect to claim 22, Kiessling discloses everything as applied to claim 21.

Additionally Kiessling discloses that the method includes exchanging data in a relatively free manner between the first storage area **(See Kiessling's figure 2(24), col.1 lines 15-21 where remote devices can access the applications on local storage)**, which defines a public data storage area, and the remote device. Kiessling discloses everything claimed as applied above to claim 21, except for explicitly reciting the use of a private storage area with which selected remote devices exchange data in a restricted manner. In analogous art, Proust et al. discloses the use of a private area with which selected remote devices exchange data in a restricted manner **(See Proust's figure 1(8), col.11 lines 14-18, figure 3 col.11 lines 41-47, col.12 lines 30-38, figure 4 col.12 lines 39-67, col.13 lines 1-11).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by including a separate data storage area for storing restricted data where access to this data is controlled in order to improve security of data, as taught by Proust et al. **(See Proust's col.3 lines 22-31).**

With respect to claim 23, Kiessling discloses everything as applied to claim 21. Additionally Kiessling discloses that the method includes
filtering requests for substantive communications from each of the remote devices with the portable device; and selectively rejecting and accepting the requests in response to the nature of services offered by the remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 24, Kiessling discloses everything as applied to claim 22.

Additionally Kiessling discloses a method that defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 25, Kiessling discloses everything as applied to claim 24. Additionally Kiessling discloses that the access rights are inherently dependent upon a classification of the remote device by the portable device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40 Kiessling does not randomly restricts access and this restriction must inherently be based on a criteria)**.

With respect to claim 26, Kiessling discloses everything as applied to claim 22. Additionally Kiessling discloses that the method includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area **(See Kiessling's col.3 lines 17-20, claim 2 col.7 lines 34-37)**.

With respect to claim 27, Kiessling discloses everything as applied to claim 22. Additionally Kiessling discloses that the method includes inherently restricting the amount of data which is writable by the remote devices into the public storage area **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21).**

With respect to claim 28, Kiessling discloses everything as applied to claim 22.

Additionally Kiessling discloses that the method includes selectively clearing data in the public storage area **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21).**

With respect to claim 29, Kiessling discloses everything as applied to claim 21 including use of security protocol (figure 2 (39), col.5 lines 10-15). However, Kiessling does not specifically recite the use of a SSL (Secure Sockets Layer). The applicant, however, has admitted the use of SSL protocol was well known and expected in the art for the purpose of securing communication lines **(See applicant's specification page 7 lines 17-19)**. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by using the well known SSL protocol as the security protocol for Kiessling's mobile device, for the purpose of enabling secure communication as admitted by the applicant.

With respect to claim 31, Kiessling discloses everything as applied to claim 21. Additionally Kiessling discloses that the method includes communicating via a radio frequency (RF) transceiver using a standardized communication protocol **(See Kiessling's figure 2(30 &31), col.4 lines 34-48).**

With respect to claim 32, Kiessling discloses everything as applied to claim 31. Additionally Kiessling discloses that the method includes communicating using technology selected from the group including Bluetooth 802.15 technology, IEEE 802.11 a technology and IEEE 802.1 Ib technology **(See Kiessling's figure 2(31), col.4 lines 34-48).**

With respect to claim 34, Kiessling discloses everything as applied to claim 21. Additionally Kiessling discloses that data is exchanged in a relatively free manner between the first storage area**(See Kiessling's figure 2(24), col.1 lines 15-21 where remote devices can access the applications on local storage)**, which defines a public data storage area, and the remote device, Kiessling discloses everything claimed as applied above to claim 34, except for explicitly reciting the use of a private storage area with which selected remote devices exchange data in a restricted manner. In analogous art, Proust et al. discloses the use of a private area with which selected remote devices exchange data in a restricted manner **(See Proust's figure 1(8), col.11 lines 14-18, figure 3 col.11 lines 41-47, col.12 lines 30-38, figure 4 col.12 lines 39-67, col.13 lines 1-11).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by including a separate data storage area for storing restricted data where access to this data is controlled in order to improve security of data, as taught by Proust et al. **(See Proust's col.3 lines 22-31).**

With respect to claim 35, Kiessling discloses everything as applied to claim 33. Additionally Kiessling discloses that the requests for substantive communications from each of the remote devices with the portable device are filtered, the requests being selectively rejected and accepted in response to the nature of services offered by the remote device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 36, Kiessling discloses everything as applied to claim 33.

Additionally Kiessling discloses defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40)**.

With respect to claim 37, Kiessling discloses everything as applied to claim 36. Additionally Kiessling discloses that the access rights are dependent upon the classification of the remote device by the portable device **(See Kiessling's figure 2(25 & 29), col.5 lines 17-40 Kiessling does not randomly restricts access and this restriction must inherently be based on a criteria)**.

With respect to claim 38, Kiessling discloses everything as applied to claim 34. Additionally Kiessling discloses requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area **(See Kiessling's col.3 lines 17-20, claim 2 col.7 lines 34-37)**.

With respect to claim 39, Kiessling discloses everything as applied to claim 34. Additionally Kiessling discloses restricting how often and the amount of data which is writable by the remote devices into the public storage area **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21)**

With respect to claim 40, Kiessling discloses everything as applied to claim 34. Additionally Kiessling discloses selectively clearing data in the public area **(See Kiessling's col. 5 lines 10-15, figure 2(25 &23), col.4 lines 15-18, col.1 lines 15-21).**

With respect to claim 41, Kiessling discloses everything as applied to claim 1 including use of security protocol **(figure 2 (39), col.5 lines 10-15).** However, Kiessling

does not specifically recite the use of a SSL (Secure Sockets Layer). The applicant, however, has admitted, the use of SSL protocol was well known and expected in the art for the purpose of securing communication lines **(See applicant's specification page 7 lines 17-19)**. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by using the well known SSL protocol as the security protocol for Kiessling's mobile device, for the purpose of enabling secure communication as admitted by the applicant.

9. Claims 9, 13, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiessling et al. (US 6,901,251) in view of Fifield (US 6,744,752).

With respect to claim 9, 13, 31, and 42, Kiessling discloses everything claimed as applied above to claim 1, except for explicitly reciting the use of Universal Plug and Play (UPnP). In analogous art, Fifield discloses the use of Universal Plug and Play **(See Fifield's abstract, col.1 lines 8-15, lines 38-48).** It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the invention of Kiessling by implementing the known plug and play protocol in Kiessling's mobile device in order to give it the capability of being attached to a local network, as taught by Fifield.

10. Claims 14, 16 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kiessling et al. (US 6,901,251) in view of well-known prior art (MPEP 2144.03).

With respect to claim 14, Kiessling discloses everything as applied to claim 1. Kiessling does not specifically disclose a rechargeable power supply for powering its various components. However, an official notice is taken that the concept and use of rechargeable battery are well known and expected in the art. Therefore, it would be obvious to one of ordinary skill in the art to modify the invention of Kiessling by incorporating a rechargeable battery as its power source.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

12. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sayed T. Zewari whose telephone number is 571-272-6851. The examiner can normally be reached on 8:30-4:30.

14. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester G. Kincaid can be reached on 571-272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

15. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sayed T Zewari/
Examiner, Art Unit 2617
August 20, 2009

/Lester Kincaid/
Supervisory Patent Examiner, Art Unit 2617